IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	)	Group Art Unit: **2132**
	)	
Shinako Matsuyama, et al.	)	Examiner: **Benjamin E. Lanier**
	)	
Application No. **09/843,403**	)	
	)	
Filed: **April 26, 2001**	)	
	)	

For: ACCESS CONTROL SYSTEM, ACCESS CONTROL METHOD, DEVICE, ACCESS CONTROL SERVER, ACCESS-CONTROL-SERVER REGISTRATION SERVER, DATA PROCESSING APPARATUS, AND PROGRAM STORAGE MEDIUM

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPELLANTS' APPEAL BRIEF

Enclosed in triplicate is Appellants' Appeal Brief for the above-referenced United States Patent Application. Appellants believe that the Brief is in full compliance with 37 C.F.R. § 1.192(c).

Applicant petitions the Commissioner for Patents to extend the time for filing the Appeal Brief by one month(s) for a fee of $120.00 so that the period for response is extended to September 30, 2005 under 37 C.F.R. § 1.136. The enclosed credit card payment form in the amount of $620.00 includes the $500.00 fee for the filing the Appeal Brief.

The Commissioner is hereby authorized to charge the extension fee and any additional

fees which may be required, or to credit any overpayment to Account No. 19-3140. **A duplicate**

of this sheet is enclosed.

Respectfully submitted,

Dated: <u>September 29, 2005</u>   By:
Marina N. Saito
Registration No. 42,121
SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. Box 061080
Wacker Drive Station, Sears Tower
Chicago, Illinois 60606-1080
(312) 876-8000

OCT 0 3 2005

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:)   Group Art Unit: **2132**
)
Shinako Matsuyama, et al.)   Examiner: **Benjamin E. Lanier**
)
Application No. **09/843,403**)
)
Filed: **April 26, 2001**   )
)
For: ACCESS CONTROL SYSTEM, ACCESS CONTROL)
      METHOD, DEVICE, ACCESS CONTROL SERVER,)
      ACCESS-CONTROL-SERVER REGISTRATION)
      SERVER, DATA PROCESSING APPARATUS, AND)
      PROGRAM STORAGE MEDIUM)

> I hereby certify that this document is being deposited with the United States Postal Service as first class mail in an envelope addressed to: MAIL STOP APPEAL BRIEF - PATENTS, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on September 29, 2005.
>
> _Antonietta Musto_
> Antonietta Musto

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

10/04/2005 SHASSEN1 00000050 09843403
01 FC:1251   120.00 OP
02 FC:1402   500.00 OP

APPELLANT'S BRIEF ON APPEAL

Dear Sir:

In accordance with the provisions of 37 C.F.R. § 1.192, Appellant herewith submits this

Brief in support of the Appeal for the above-referenced application.

I.   REAL PARTY IN INTEREST

The real party in interest in the present appeal is the Assignee, Sony Corporation, a

Japanese Corporation. The Assignment was recorded in the U.S. Patent and Trademark Office at

Reel 012101, Frame 0759.

II.   RELATED APPEALS AND INTERFERENCES

There are no related appeals and no related interferences.

III.   STATUS OF CLAIMS

Claims 1-2, 4-6, 8-15, 17-18, and 20-25 are pending in this application.   The present

Appeal is directed to claims 1-2, 4-6, 8-15, 17-18, and 20-25 which were finally rejected under

35 U.S.C. § 102(e) as being anticipated by Doyle (U.S. Patent No. 6,128,738) and under 35

U.S.C. § 103(a) as being obvious based Doyle in view of Misra (U.S. Patent No. 5,757, 920) in a

final office action dated March 1, 2005.

IV.   STATUS OF AMENDMENTS

There are no pending amendments.   However, appellants reserve the right to submit an

amendment to correct noted typographical errors that do not affect the appeal.

V.   SUMMARY OF INVENTION

The present invention is directed to an access control system for use in a data transfer

system which transfers data by means of public-key cryptosystem based on a public key

certificate issued to an authentication object by a public key issuer authority.   The access control

system comprises a service provider, a service receiving device, an access control server, and a

system holder.   The service provider is an authentication object and which provides services.

The service receiving device also is an authentication object and receives services provided by

the service provider.   The access control server issues to the service receiving device an access

permission, which identifies a service provider an access to which by the service receiving

device is permitted.   The system holder is an organization that provides or controls contents

usable by a user terminal, contents which enables provision of services, or a service distribution

infrastructure. The service provider performs, based on the access permission, a decision as to whether an access request by the service receiving device is to be permitted. The system holder is configured to administrate the service provider and the service receiving device and to treat the service provider and the service receiving device as authentication objects and generates the access permissions in a form independently usable for the service provider.

VI.   ISSUES

The issue on Appeal is as follows:

1.   Whether claims 1-2, 4-6, 8-13, 15, 17-18, and 20-24 are anticipated by Doyle; and

2.   whether claims 14 and 25 are obvious over Doyle in view of Misra.

VII.   GROUPING OF CLAIMS

Based on the rejection set forth by the Examiner, claims 1-2, 4-6, 8-15, 17-18, and 20-25 stand or fall together. Appellant, however, reserves the right to pursue the claims separately in any continuation application.

VIII.   ARGUMENT

Claims 1-2, 4-6, 8-15, 17-18, and 20-25 are patentable over Doyle.

A.   The Claimed Invention

Claim 1 is directed to an access control system for use in a data transfer system which transfers data by means of public-key cryptosystem based on a public key certificate issued to an

authentication object by a public key issuer authority. The access control system comprises a service provider, which is an authentication object and which provides services, a service receiving devices, which also is an authentication object and which receives services provided by the service provider, and an access control server which issues to the service receiving device an access permission, which identifies a service provider an access to which by the service receiving device is permitted. The system holder which is an organization that provides or control contents usable by a user terminal, contents which enables provision of services, or a service distribution infrastructure. The service provider performs, based on the access permission, a decision as to whether an access request by the service receiving device is to be permitted and the system holder is configured to administrate the service provider and the service receiving device and to treat the service provider and the service receiving device as authentication objects and generates the access permissions in a form independently usable for the service provider.

Claims 2, 4-6, and 8-14 depend from claim 1.

Claim 15 is directed to an access control method for use in a data transfer system which transfers data by means of public-key cryptosystem based on a public key certificate issued to an authentication object by a public key issuer authority. The access control method comprising the steps of receiving, at a service provider, an access permission from a service receiving device, the access permission having been issued by a service control server; and executing, based on the access permission, a determination as to whether access requested by the service receiving device is to be permitted. Issuing at a issuing step for issuing, at an access control server, an access permission which is delivered to the service receiving device and which enables

identification of the service provide an access to which is permitted by the service receiving device wherein the access control server generates the access permission in a form commonly usable for a plurality of service providers.

Claim 17-18 and 20-25 depend from claim 15.

B.   Claims 1-2, 4-6, 8-15 and 20-25 are patentable over Doyle

In the Final Office Action, claims 1-2, 4-6, 8-13, 15, 17-18, and 20-24 were rejected under 35 U.S.C. § 102(e) as being anticipated by Doyle (U.S. Patent No. 6,128,738), and claims 14 and 25 were rejected under 35 U.S.C. § 103(a) as obvious over Doyle in view of Misra (U.S. Patent No. 5,757,920).   The Examiner has not made an adequate showing to support his rejections.

Doyle discloses a method and system for enabling a single client certificate to be used in SNA communication to ensure security such that the certificate cannot be intercepted or reused. (See Abstract). In Doyle, when the host receives the information about which host application is selected, the host application provides the information and a bind request 307 is sent from the host to the client. The client responds with a bind response 309. The host application then sends a request to the client for their certificate 311. The client responds by creating a security packet and sending the security packet to the host 313 for authentication. The host application forwards the client's certificate to a host access control 315. Once authenticated, the host access control returns a response to the host application 317. At that point, logon is complete and application data begins to flow 319 between the client and the host application. (Col. 5, line 67 - Col. 6, line 14). Thus, both the client and host application are required to store and administrate various

kinds of data for authentication, increasing the load on each device. The Examiner stated Doyle at Col. 1, line 66 - Col. 2, line 15 discloses that the certificates and signatures created are usable for a plurality of services. Contrary to the Examiner's statement, however, in Doyle, the series of steps detailed above must be repeated whenever the user attempts to access any other application or system of the host. (See Col. 4, lines 15-21). This represents prior art over which Applicants' present invention is an improvement as Doyle requires distinct configuration and authentication for each host application and the present invention does not. (See Id. and Col. 5, lines 48-58). Thus, Doyle does not disclose or suggest generation of the access permissions in a form independently usable for the service provider as required by claim 1. For similar reasons to those explained for claim 1, the remaining claims 2, 4-6, 8-15, 17-18, and 20-25 are also allowable over Doyle . Moreover, because Doyle does not disclose or suggest generation of the access permissions in a form independently usable for the service provider, it would not have been obvious to one skilled in the art at the time of invention to modify the system/method disclosed by Doyle, with the teaching of Misra to generate claim 14, which depends from claim 1, or to derive claim 25, which depends from claim 15.

In view of the foregoing, Appellant respectfully submits that claims 1-2, 4-6, 8-15, 17-18, and 20-25 are patentable and the application is in condition for allowance.

C.   Conclusion

Appellant respectfully submits that the subject matter of the claims on appeal is not found or suggested by Doyle. Thus, the Examiner has not made an adequate showing of anticipation with respect to the subject matter of the rejected claims. Appellants, therefore, respectfully

request reversal of the Examiner's decision to reject claims 1-2, 4-6, 8-15, 17-18, and 20-25

under 35 U.S.C. § 102(e) and claims 14 and 25 under 35 U.S.C. § 103(a) as being unpatentable

over Doyle, and respectfully request allowance of all pending claims.

Respectfully submitted,

Dated: September 29, 2005   By: _____

Marina N. Saito
Registration No. 42,121
SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. Box 061080
Wacker Drive Station, Sears Tower
Chicago, Illinois 60606-1080
(312) 876-8000

IX.   APPENDIX

1.   (Previously Presented) An access control system for use in a data transfer system which transfers data by means of public-key cryptosystem based on a public key certificate issued to an authentication object by a public key issuer authority, the access control system comprising:

a service provider which is an authentication object and which provides services;

a service receiving device which also is an authentication object and which receives services provided by the service provider; and

an access control server which issues to the service receiving device an access permission which identifies a service provider an access to which by the service receiving device is permitted;

a system holder which is an organization that provides or controls contents usable by a user terminal, contents which enables provision of services, or a service distribution infrastructure;

wherein the service provider performs, based on the access permission, a decision as to whether an access request by the service receiving device is to be permitted; and

the system holder is configured to administrate the service provider and the service receiving device and to treat the service provider and the service receiving device as authentication objects and generates the access permissions in a form independently usable for the service provider.

2.   (Original) An access control system according to Claim 1, further comprising:

an access-control-server registration server,

wherein the access-control-server registration server is configured to execute a processing for requesting the access control server to execute issuance of the access permission, upon receipt of an access permission issuance request from the service receiving device.

3.   (Cancelled).

4.   (Previously Presented) An access control system according to Claim 1, wherein a plurality of the system holders are provided, and wherein the access control server is provided for each of the system holders and is configured to issue the access permission in regard to the services provided by the service provider administrated by the system holder.

5.   (Previously Presented) An access control system according to Claim 1, wherein a single access control server is provided commonly for a plurality of system holders, and is configured to issue access permissions in regard to the services provided by the service provider administrated by the system holders.

6.   (Previously Presented) An access control system according to Claim 1, further comprising a root registration authority which administrates the system holder, wherein the root registration authority .is configured to execute, based on a request from the system holder, a processing to request the public key certificate issuer authority to issue the public key certificates of the authentication objects administrated by the root registration authority.

7.   (Cancelled).

8.   (Original) An access control system according to Claim 1, wherein the access control server generates the access permission in a form commonly usable for a plurality of service providers.

9.   (Previously Presented) An access control system according to Claim 1, wherein the system holder is configured to generate the access permission in a format which comprises:

an access-control-server-set fixed field set by the access control server;

a service-provider-set option field set by the service provider; and

an electronic signature field to be performed by the access control server.

10.   (Previously Presented) An access control system according to Claim 9, wherein the service-provider-set option field includes identification data which indicates for the service receiving device whether an access by the service receiving device is permitted, and wherein the identification data includes at least one of personal information concerning the user of the associated service receiving device, user ID, user device ID, and an access permission discrimination flag.

11.   (Original) An access control system according to Claim 1, wherein the data transfer between the service provider, the service receiving device and the access control server, performed directly or indirectly through an intermediary, is executed on condition that mutual authentication has been established between the sender of the data and the receiver of the data.

12.   (Original) An access control system according to Claim 1, wherein the data transfer between the service provider, the service receiving device and the access control server, performed directly or indirectly through an intermediary, transfers the data with an electronic signature of the sender added thereto.

13. (Original) An access control system according to Claim 1, wherein the service provider is a device which provides a service.

14. (Original) An access control system according to Claim 1, wherein the access control server is configured to execute an access permission changing processing for revocation of the permission set on the access permission.

15. (Previously Presented) An access control method for use in a data transfer system which transfers data by means of public-key cryptosystem based on a public key certificate issued to an authentication object by a public key issuer authority, the access control method comprising the steps of:

receiving, at a service provider, an access permission from a service receiving device, the access permission having been issued by a service control server;

executing, based on the access permission, a determination as to whether access requested by the service receiving device is to be permitted; and

issuing, at an access control server, an access permission which is delivered to the service receiving device and which enables identification of the service provide an access to which is permitted by the service receiving device, wherein the access permission issuing step generates the access permissions in a form independently usable for each of the service providers.

16. (Cancelled).

17.   (Original) An access control method according to Claim 15, further comprising the steps of:

receiving, at an access-control-server registration server, the access permission issuance request from the service receiving device and requesting, at the access-control-server registration server, the access control server to execute the processing for issuing an access permission.

18.   (Original) An access control method according to Claim 15,

wherein the access permission issuing step is executed based on an issuance request from a service provider which is under the administration of a system holder as an organization that provides or controls contents usable by a user terminal, contents which enables provision of services, or a service distribution infrastructure.

19.   (Cancelled).

20.   (Original) An access control method according to Claim 15, wherein the access control server generates the access permission in a form commonly usable for a plurality of service providers.

21.   (Previously Presented) An access control method according to Claim 15, wherein the access permission issuing step generates the access permission of a format which comprises:

an access-control-server-set fixed field set by the access control server;

a service-provider-set option field set by the service provider; and

an electronic signature field to be performed by the access control server.

22.   (Previously Presented) An access control method according to Claim 15, wherein the step executed by the service provider for determining whether the access is to be permitted is executed based on identification data which determines whether the access is to be permitted for the service receiving device and which is contained in the access permission, the identification data including at least one of personal information concerning the user of the associated service receiving device, user ID, user device ID, and an access permission discrimination flag.

23.   (Original) An access control method according to Claim 15, wherein the data transfer between the service provider, the service receiving device and the access control server, executed directly or indirectly through an intermediary, is executed on condition that mutual authentication has been established between the sender of the data and the receiver of the data.

24.   (Original) An access control method according to Claim 15, wherein the data transfer between the service provider, the service receiving device and the access control server, executed directly or indirectly through an intermediary, transfers the data with an electronic signature of the sender added thereto.

25.   (Original) An access control method according to Claim 15, further comprising an access permission changing processing executed by the access control server to revoke the permission set on the access permission.

26-42. (Cancelled).